

Abstract

A security module, a personalization unit and a method for use thereof, where the security module contains a secret key from a key pair for asymmetrical encryption, and the personalization unit produces a certificate about the public key from the key pair and sends it to the security module together with the public key from a central system. The security modules uses this certificate and the public key to protect the communication with a central system, particularly in the field of banking.

Figure 1